Widening Your Secure eBusiness to Wireless

Broadening the Security Umbrella to Include Wireless Devices

An IDC White Paper
Sponsored by Tivoli Systems Inc.

Roseann Day and John Daly With Tim Sheedy and Chris Christiansen
December 2000

Introduction

The promise of pervasive access to data and computing resources seems close to reality. The current availability of a wide range of affordable, portable devices can open up vast new opportunities for wireless Internet access. IDC estimates that the worldwide market for wireless Internet transactions will grow to $38 billion by 2003.

Voice traffic will still comprise much of the wireless transmission growth. However, IDC forecasts that in the next three years, data over wireless TCP/IP will account for 55% of wireless transmission. The potential to reach a broad base of both consumers and business users makes wireless applications appealing to businesses investing in online ebusiness initiatives. However, wireless access raises security challenges beyond those normally encountered with wireline business on the Internet.

This paper reviews how leading adopters of wireless Internet have approached these security challenges. It shares how these firms aim to simplify the execution of corporate security policy in the wireless context. The paper also takes a look at Tivoli's approach to simplifying the challenge of deploying wireless Internet applications that support and integrate corporate security policy.

Methodology

IDC developed this report using a combination of direct primary research, wide-scale quantitative customer surveys, and wireless and security market forecasts. To understand the most important security issues challenging wireless ebusiness initiatives, we selected seven corporations that were actively extending their ebusiness initiatives to

IDC
Analyze the Future

5 Speen Street • Framingham, MA 01701 • Phone (508) 872-8200 • Fax (508) 935-4015

include wireless access. These organizations operated in financial services, transportation, travel services, and gaming industries — the segments most actively extending wireless Internet access. We conducted in-depth qualitative discussions with these organizations, exploring the particular issues and challenges they found most pressing. This report reflects all of these research perspectives.

Wireless eBusiness

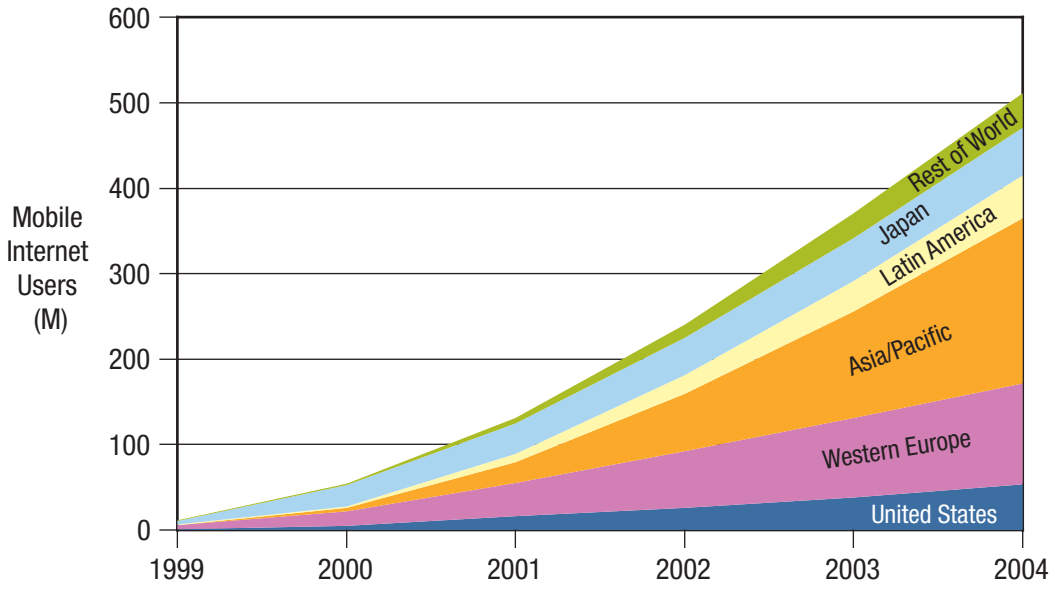
The Potential

The number of Internet users worldwide continues to grow at a phenomenal rate. IDC estimates that the worldwide Internet user population will almost double between 1999 and 2003, growing from 240 million to 602 million users. That growth rate pales, however, in comparison to the expected increase in the number of wireless Internet access users. Though voice continues to drive mobile use, we find strong growth in subscribers with some level of Internet access.

Japan, where small mobile devices of all types have received early acceptance, has become a leader in end-user acceptance of mobile voice and data access. The Japanese Ministry of Posts and Telecommunication estimated the number of mobile Japanese users at 55 million in August 2000. IDC estimates that more than 21 million of those access the Internet today. In Western Europe, where wireless telephony addressed basic consumer needs for more extensive voice access, penetration matches Japan with more than 17 million wireless Internet users today. In China, more than 65 million wireless telephones and personal digital assistants (PDAs) operate already, and widespread use is just beginning. Figure 1 presents IDC's preliminary estimates of growth in mobile Internet users worldwide. This worldwide growth potential — more than 100% compounded annually — has generated interest in potential wireless ecommerce and ebusiness opportunities, among a wide range of industries.

These numbers certainly appeal to enterprises across a wide range of industry sectors seeking additional customers and users. But expansion of ebusiness to wireless does not always occur easily. We have found wireless Internet access involves a different set of technical, user interface, and security constraints from those found in traditional Internet-enabled environments. The leaders in wireless Internet access are just uncovering some of these challenges.

Figure 1
Worldwide Growth in Mobile Internet Users — Preliminary Estimates



Source: IDC, 2000

Background: The Realities of Wireless Internet Applications Today

Several earlier adopters of wireless Internet solutions spoke of a variety of the challenges they encountered launching wireless Internet applications. Our discussions with them focused on the business and technical challenges affecting security for wireless Internet access. They highlighted some of the limits of current technologies supporting wireless Internet. Most of the sites described the technology environment supporting secure wireless Internet access as in its formative stages and "still taking shape."

Wireless Application Protocol Promise vs. Practice

These early adopter perspectives identifying some of the limits to the technology arose despite aggressive vendor efforts to advance the technology. Any discussion of security for wireless Internet access requires a review of wireless application protocol (WAP) initiatives — the vendors' efforts to create a standards-based environment for secure wireless Internet business growth. The major vendors in the wireless space have attempted to shape directions for wireless Internet applications through the WAP Forum. The Forum hopes to facilitate the development of applications for WAP devices by proposing standards for the applications programming interfaces. Other cross-vendor efforts are also attempting to facilitate easier use of mobile devices. For example, the SyncML initiative proposes an open industry specification for universal data synchronization (i.e., synchronization of remote data and personal information across multiple networks, platforms,

and devices). Additionally, technologies, such as Bluetooth — which provides short-range, wireless connectivity at high bandwidth to a variety of mobile devices — and iMode — a burgeoning standard for mobile Internet access originating in Japan — amplify the growth potential for mobile.

Recognizing the importance of security in the wireless environment, the forum has also endorsed a protocol to increase the security of wireless transmissions, Wireless Transport Layer (WTLS). WTLS is the wireless version of the industry standard Transport Layer Security (TLS). TLS provides a secure network connection session by providing cryptographic protection to the communications between the client and a server. In wireless Internet applications, this link operates via a secure link established between the browser on the WAP-enabled device and a Web server. WTLS protects the data from being read in transit and ensures its integrity while being sent. This security process works most effectively when combined with tight authentication and authorization mechanisms to restrict access to specific resources by only authorized users.

At the start of 2000, the WAP Forum and the WTLS protocol received a lot of attention from vendors and the press alike. It reached a level of coverage as one of the hot technologies of the year. However, by summer of 2000, it became clear that the actual deployment of wireless Internet applications was falling well short of early marketing predictions. Competing security approaches to wireless Internet may be contributing to the lag. For example, an alternative approach for securing mobile devices, GSM phones with Smartcard authentication, is achieving some acceptance with the application community. Deutsche has teamed with Nokia, Barclaycard with Cellnet, and Telia with Postgirot to create mobile banking applications.

Wireless Internet Clients

At this developmental stage of the wireless Internet market, devices used for wireless access have taken their first steps toward Internet readiness. Integrated wireless modems in PDAs and laptops, two-way paging, and improved graphical displays on devices are becoming more common and affordable. The highly variable usability options of these various devices (keyboards, stylus, display size) impose sharply different options for accessing data as well as voice. The variability makes establishing wireless Internet access standards more difficult.

A Different Web Experience

Wireless Internet access changes the style of user interaction with the Web. Traditional Web access can exploit the power of desktop and even TV video units displaying rich graphical environments. CPU-power-impaired wireless devices, on the other hand, cannot act as traditional browsers. The wireless Internet access experience leaves out the graphics but provides the textual data because the devices cannot

support inefficient displays. Access to Internet-based data via wireless devices can therefore seem fast and simplified. In some cases, end users may not even be aware that wireless data is coming to them from the Internet because they are likely to be focused on the data rather than its transmission. As one executive of a wireless application provider explained, "When you go to a destination site on the Web, the vast majority of the content being displayed is going to be heavily graphical, and most of it has no relevance to what you're interested in. I call it an attention tax. You're getting free content, but you're paying for it with your attention and time."

Directions for Growth

Fast, simple, and ubiquitous access makes wireless Internet usage appealing across a wide range of industries that rely on workers and customers who are typically on the move. Sales, field service activity, distribution, inventory tracking, and transportation all reap immediate benefits from wireless data access.

Additionally, companies in industries that rely on service extension for customer loyalty, such as financial services and travel, feel compelled to extend wireless access to their customers. As one ebusiness manager put it: "The major driver is the competitive nature in the world. We're trying to get people to be more efficient and spending more time out of the office but still having huge access to corporate information." For a variety of industry segments — including travel, financial services, and media — wireless Internet initiatives are being launched worldwide. The cost of not doing business in the wireless world might mean lost market share. Therefore, for some, time to market outweighs many cost considerations. One of the travel companies interviewed described it as a corporate investment in better usability and the business as a whole. They had not done a true cost/benefit analysis.

Travel-related and financial services have been among the first to extend their applications and include wireless access. Early feedback indicates that online banking information, travel schedule data, weather forecasts, and travel directions data provide great value to mobile users. These types of data — textual, factual, and compact — work effectively with wireless devices. They ship swiftly to any location and offer value even without added graphical content or audio content. Enhanced audio and graphical content will certainly follow as the devices themselves are enhanced, but applications that do not depend on "such bit-heavy" data will be first to gain share, leading the initial wave of use.

Telecommunications companies are anticipating immense savings in customer care and billing as they contemplate ecare and ebill wireless applications. eCare would provide automated voice responses to repeated customer service questions. eBilling will deliver telecom bills directly to one's wireless handset.

Obstacles to Overcome

Despite the advantages, deployment of wireless Internet applications has not met early forecasts. Some of the lag might simply reflect the early hyperbole that surrounded the technology. However, other factors might play into the slower market uptake. Some U.S. consumers, used to highly graphical and easily navigated experiences of the Web, find limited, text-based Web interfaces disappointing and cumbersome to traverse. Usability features are likely to slow adoption until both the devices and the applications using them become more appealing for Web access.

In marketplaces such as China and Latin America, where WAP-enabled phones and PDAs may be users' first chance to interact with Web content, the potential seems greater and sales are taking off.

Although wireless Internet applications are taking off more gradually than early marketing might have forecast, the trend toward more ubiquitous access to corporate data via the Internet will grow as wireless device technologies, bandwidth, and security improve. IDC's European mobile data forecast expects European carrier revenue from WAP data to start slowly but then increase at over 100% compound annual growth from 2000 to 2004. IDC's forecasts reflect the time needed for more wireless Internet applications to come online and for WAP-enabled devices to mature in usability features.

Security for Wireless Internet Access

Security for wireless Internet applications poses new challenges to ebusiness managers. Securing data and transactions from the wireless device, through the air, through the carrier links, over the Internet, and onto the protected server involves bringing together security issues at multiple levels. The issues arise from the devices themselves, at the network level, and across the global enterprise.

Security at the Device Level

By definition, mobile devices are small and highly portable. Their light weight and small size make them easy to carry but also easy to misuse. Because of their mobility and portability, the devices suffer more instances of theft, breakage, and ready access by people other than the assigned owner of the device. When improperly authenticated, they can offer an outsider ready access to crucial corporate data.

These vulnerabilities can be annoying for individual owners. For a large enterprise that may have invested in hundreds of thousands of mobile units for its employees or partners, these vulnerability issues scale to an enormous management liability. For enterprises engaging in large ecommerce sites or in global ebusiness partnerships that involve vast numbers of devices, the problems can become overwhelming. One bank indicated that it felt particularly uncomfortable about extending

the range of online banking functions to its more than 10,000 wireless customers until it could better assure client authenticity.

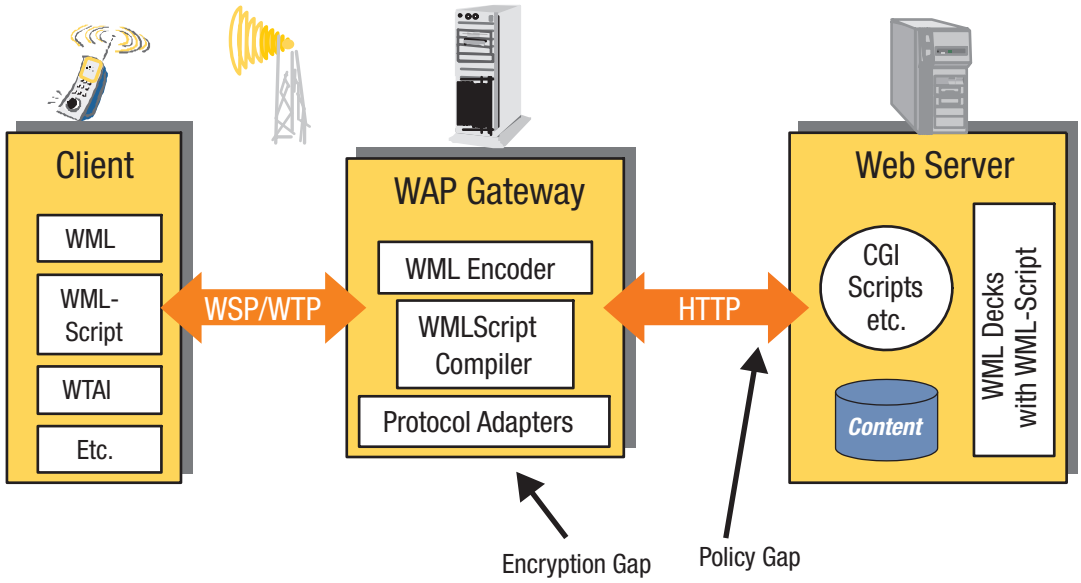
Protection of data sent from the client can pose problems as well. Handheld devices operate at a fraction of the CPU power of a standard PC. For example, a new PalmVII has 8MB of memory, while most desktops are shipped with 128MB or more. This memory limitation and the finite battery life hamper mobile devices' ability to handle processing-intensive encryption for every communication. Robust but lightweight encryption technologies suitable for such devices are now available. However, these technologies are just beginning to appear in the applications and infrastructures required for securing sensitive wireless applications.

Security Between the Wireless Device and the Internet

The small, highly portable nature of wireless devices poses security problems. In addition, the multimode nature of the link between the wireless device and its eventual network destination adds more exposure. Most wireless service providers cover wireless security in two steps: First, for the wireless leg of the journey, the communicating node (client or wireless gateway) encrypts the transmitted packets to shield them for privacy. Second, after the packets are delivered to the wireless gateway, the transmissions briefly become unencrypted and examined so that they can be routed after their re-encryption (see Figure 2).

This design thus creates an "encryption gap" at the wireless gateway, which could be exploited to snoop transactions during the brief point of decryption. Though fixes for this gap are coming to market in the version of WAP due out in early 2001, early adopters recognize the current exposure. To handle this issue for the near term, these enterprises have negotiated careful service agreements with the carriers that manage the gateways, launched less-sensitive applications first, and/or placed wireless gateways within their trusted network.

Figure 2
Wireless Internet Pathway



Source: Diagram - WAP Forum; 'Gap' Overlays - IDC, 2000

Security Gap Potentials

Security Between the Wireless Internet Gateway and the Enterprise

Security certainly doesn't end with the devices and the carriers. The enterprise itself and its management of wireless access completes the picture of overall security. If corporate security policy does not consistently extend from the wired world to wireless access, it leaves an architectural or policy security "gap." Whereas corporations must await fixes to the encryption "gap," they can manage this wireless policy gap themselves.

Security Risks and Implications

Wireless Internet demands a new way of planning for security that recognizes from the start the vulnerabilities inherent in wireless access. Because wireless security involves a two-step encryption and re-encryption process, it cannot assure true end-to-end security in the current form. The current wireless Internet access environment also lacks tight user authentication at the device. Finally, the physical mobility of the devices themselves increases the need to tighten security. Future releases of technology and improved WAP and other standards will address these vulnerabilities, but they exist today.

Before new versions of the WAP protocol and technology upgrades reach the market, organizations face constraints in securing wireless Internet solutions. Attempting to address the inherent vulnerabilities by patching or reworking an existing Internet solution will prove awkward at minimum. More likely, patch approaches to improve security will introduce complexities and vulnerabilities of their own. A more appropriate model of trust should begin with addressing the vulnerabilities intrinsic to wire-

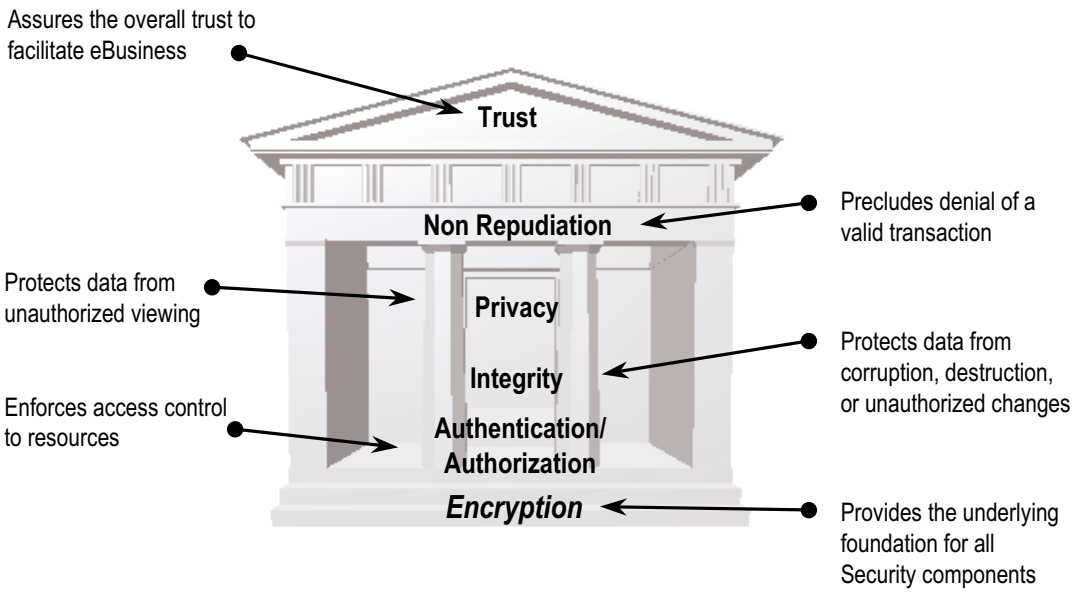
less computing and conducting ebusiness transactions best suited to the current constraints.

Managing Wireless Internet Securely

Wireless Internet access offers the potential for immense process efficiencies, wider markets, and better customer service. The attraction and the pressure to compete over the wireless Internet seem intense. However, the basics of IT security still apply and force a balanced approach. The fundamentals of good policy, basic physical security, strong authentication and access control, and ongoing management and audit have shaped effective security in the pre-Internet, post-Internet, and now, wireless business marketplaces.

As with any other enterprise initiative, organizations should approach wireless ebusiness initiatives with a secure building-block approach that creates a protected "whole" from secure components (see Figure 3).

Figure 3
Fundamental Secure Wireless Components



Source: IDC, 2000

The Foundation: Policy

Effective security begins with articulating the policies for access to enterprise assets — equipment, data, and applications. This articulation defines proper business use of all asset types by different types of enterprise users. Policy dictates *which* corporate assets are protected, *who* can access which assets, and *why* users should have that access in case of exceptions and modifications.

For wireless ebusiness, enterprise access policies become even more important because of the scale of the challenges. By design, mobile devices increase the number of devices per user — increasing the policy management task. Wireless devices also widen accessibility into the corporate computing environment. This means that the numbers of discrete assets and users to be managed increases exponentially. It also means that threats to the enterprise scale accordingly.

Reasonable wireless security planning addresses this scale problem from the start. Appropriate policy definition and management recognizes that users will have multiple devices and may use multiple Internet service provider (ISP) carriers for access to corporate data. Policy and policy oversight capabilities should take these factors into account.

Good policy planning also means recognizing that, even if the enterprise has not issued mobile devices to its employees or customers, they may well weave their way into the ebusiness fabric. The affordability and appeal of such devices means that users will own and want to use mobile devices for both work and personal reasons. During our interviews, we received feedback from industries as diverse as hospitals and banks that employees were already introducing personal mobile devices into the corporate environment. One healthcare enterprise described the pressure to support physicians' PDAs. As leading adopters of wireless acknowledge, "wireless access will be pervasive in every piece of our lives, whether we like it or not."

Integrate Security and Policy Management in the Environment

Effective policy and policy management rely in turn on application design and construction to incorporate these policy factors. Wireless applications must pay particular attention to access control, authorization checks, and authentication support. Initial designs of wireless Internet extensions must pay careful attention to controlling data and function range.

While there is no formal industry standard for security policies, many IT security products are configured according to user-defined security policy. Policy-based configuration and management supports consistency across the enterprise, which is essential to controlling access to valued enterprise assets.

Over the long term, good security design from the policy down can also contribute much to manageability, scalability, and risk management.

Getting Help: Vendors Supporting Wireless Internet Security

At the start of 2000, when media hype over Y2K was dying down, support for wireless Internet applications was the rage. The first security conferences of the year were awash in announcements of support for a variety of products to enable digital certificates for wireless and to handle encryption on small devices.

A wide range of companies made announcements in this area. Among the many vendors with offerings in the wireless Internet security space are the major systems and networking vendors, including IBM Corporation, with its Tivoli Systems software subsidiary, Cisco Systems, and the security specialty companies, including RSA Security, Axent Technology, and Network Associates. Encryption and digital certificate vendors, such as Certicom, NTRU, Entrust Technologies, and VeriSign, have also announced support for wireless Internet security.

Although WAP security is still maturing, enterprises can choose from well-established Internet security technologies that have been extended for wireless use. Most important is selecting security technologies that come with ongoing support to help enterprises grow their wireless initiatives as the devices and protocols mature.

Tivoli SecureWay and Wireless Security

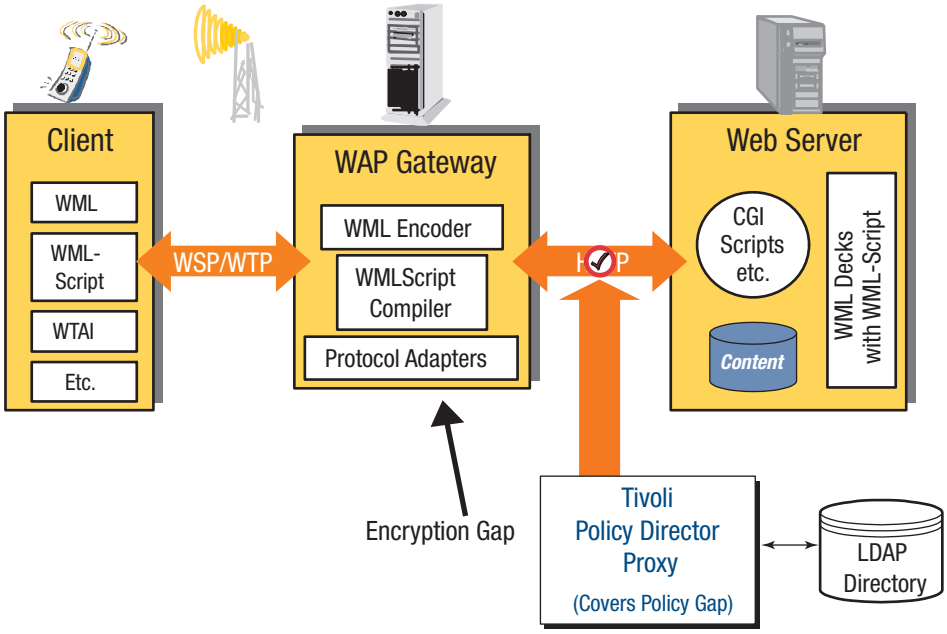
Wireless ebusiness initiatives pose the fundamental problem of security scale. Wireless Internet initiatives are integrating tens of thousands — or more — mobile devices into an existing enterprise Internet framework. Extending corporate-controlled security policy to such an exponentially expanded base of mobile users and devices requires direct advanced preparation. Dealing with the scale implications after the fact as an add-on step has caused early adopters immense difficulties. Tivoli Systems, an IBM Company, has recognized this inherent problem with wireless Internet access and extended its Tivoli SecureWay Policy Director to offer an automated and controlled method to accommodate wireless growth.

Tivoli SecureWay Policy Director is a security policy management tool that provides a secure applications portal for ebusiness and distributed applications. The software is designed to address the scalability of manageability issues in securing ebusiness sites by simplifying the implementation of enterprise policy across platforms. With increased interest in wireless connectivity for enterprise ebusiness uses, Tivoli has extended its SecureWay Policy Director to deal with the "policy gap" and facilitate both traditional and wireless access (see Figure 4).

Tivoli SecureWay Policy Director facilitates wireless access by the use of replicated proxies, which are transparently inserted between the WAP Gateway and the application server. The proxies leverage polices that control wireless users' access to data and transactions. This is exactly the same policy those users are subject to when on their traditional desktop devices.

Tivoli designed SecureWay Policy Director to tie together important security technologies under a consistent enterprisewide (i.e., including Web, distributed, and legacy environments) policy. This approach avoids deploying a patchwork of potentially conflicting policy management solutions, some of which support only the newer Web environments, others of which support only the older, traditional back

Figure 4
Tivoli's SecureWay Policy Director Authorization for Wireless



Source: Diagram - WAP Forum; Overlays - IDC, 2000

end. It also helps reduce implementation time and management complexity. Such a reduction in complexity and management overhead can reduce the total cost of secure computing.

The major components of Tivoli SecureWay Policy Director address the key security components for any secure applications portal — strong authentication and comprehensive access control, all managed centrally in such a way that the security policy for the entire wired and wireless Web environment is well understood. This product can provide centralized access control for both network policy and application security policy. It also provides fine-grained access control for Web applications without modifications to existing Web-based applications. For enterprises moving to wireless applications, Tivoli SecureWay Policy Director helps companies protect Web resources by extending central control to business applications and data accessed through WAP devices. This step can reduce the cost and complexity of extending existing ebusiness to users who have WAP-enabled cell phones, PDAs, and other handheld devices.

The simplicity of this solution supports the way mobile users access their enterprise accounts. With Tivoli SecureWay Policy Director, mobile users can access Web resources using the user names already established for their access via traditional Internet devices.

By widening Policy Director to the wireless world, Tivoli extends to that community the usability features it has been delivering to traditional users. The benefits target: "ecommunity single sign-on," scalability (via replication and load balancing), personalization, entitlements, dossier, heterogeneous Web server support, and effective linkage to enterprise servers.

Control and simplicity represent true cost benefits in the complex world of wireless ebusiness. By helping enterprises maintain centralized control while reducing the modifications required to new applications, the Tivoli SecureWay solution can reduce the costs of adding new wireless ebusiness applications to an enterprise where policy has already been set for other enterprise applications. With the potential scale for wireless ebusiness reaching millions of users on scores of applications, the cost and maintenance benefits can be impressive.

The Bottom Line for eBusiness Executives

Secure wireless Internet access is all about manageability. At the device level, at the carrier level, and at the application and enterprise level, the primary challenges are not technical. Instead, the challenges are scale and manageability.

Building a wireless global enterprise will soon be technically affordable. The ebusiness winners in this market will be those who select technology vendors that work as enterprise partners and help the enterprise grow, manage, and protect its wireless solutions.

Wireless Internet access for ebusiness will benefit enterprises with increased productivity, more extensive customer service, and tighter integration of mobile workers, suppliers, and customers. Success with wireless Internet does require two essential security management steps: (1) Planning from the start for the management of immense growth in user and device scale and (2) designing applications that recognize the unique security deficiencies of mobile devices and mobile users.

Technology, such as that offered with Tivoli SecureWay Policy Director, can help enterprises deploy wireless Internet applications both securely and efficiently. Tivoli SecureWay allows enterprises to extend enterprise policy across both wireless and wireline access. If this technology is deployed with a recognition that wireless Internet access applications need to be scaled to both the device size and the range of potential usage, Tivoli SecureWay offers a means to get to market quickly while maintaining a secure environment. This can be a winning combination for today's mobile enterprise.

NORTH AMERICA

Corporate Headquarters
5 Speen Street
Framingham, MA 01701
508-872-8200

IDC Canada
36 Toronto Street, Suite 950
Toronto, Ontario, Canada M5C2C5
416-369-0033

IDC Irvine
18831 Von Karmen Ave, Ste 200
Irvine, CA 92612
949-250-1960

IDC Mtn. View
2131 Landings Drive
Mountain View, CA 94043
650-691-0500

IDC New Jersey
120 Wood Ave South, Suite 509
Iselin, NJ 08830
732-632-9222

IDC New York
2 Park Avenue
Suite 1505
New York, NY 10016
212-726-0900

IDC Texas
100 Congress Ave, Suite 2000
Austin, TX 78701
512-469-6333

IDC Washington
8304 Professional Hill Drive
Fairfax, VA 22031
703-280-5161

ASIA/PACIFIC

IDC Asia/Pacific (Hong Kong)
12/Floor, St. John's Building
33 Garden Road
Central, Hong Kong
852-2530-3831

IDC Asia/Pacific (Singapore)
71 Bencoolen Street, #02-01
Singapore 189643
65-226-0330

IDC Australia
Level 4, 76 Berry Street
North Sydney, NSW 2060, Australia
61-2-9922-5300

IDC China
Room 611, Beijing Times Square,
88 West Chang'an Avenue, Beijing,
P.R. China, 100031
86-10-8391-3456

IDC (India) Limited
Cyber House
B-35, Sector 32 - Institutional
Gurgaon - 122002, Haryana, India
91-124-6381673 to 80

IDC Japan
10F The Itoyama Tower
3-7-18, Mita Minato-ku
Tokyo 108-0073, Japan
81-3-5440-3400

IDC Korea Ltd
Suite 704, Korea Trade Center
159-1, Samsung-Dong, Kangnam-Ku
Seoul, Korea 135-729
82-2-55-14380

IDC Malaysia
Suite 13-03, Level 13, Wisma KiaPeng
No. 3, Jalan Kia Peng
50450 Kuala Lumpur, Malaysia
6-03-2163 3715

IDC New Zealand
Level 7, 246 Queen Street
Auckland, New Zealand
64-9-309-8252

IDC Philippines
7F, SEDCCO 1Bldg
Rada Street Corner
Legaspi Street
Legaspi Village
Makati City, Philippines
632-894-4808

IDC Taiwan Ltd.
10F, 31
Jen-Ai Rd, Sec 4,
Taipei 106, Taiwan, R.O.C.
886-2-2731-7288

IDC Thailand
27 Soi Charoen Nakorn 14
Charoen Nakorn Road, Klongtonsai
Klongsan Bangkok 10600, Thailand
66-2-439-4591-2

IDC Vietnam
37 Ton Duc Thang Street
Unit 1606
District-1 Hochiminh City Vietnam
84-8-910-1235

EUROPE, MIDDLE EAST, AND AFRICA

IDC Austria
c/o Loisel, Spiel, Zach Consulting
Mayerhofgasse 6
A-1040 Vienna, Austria
43-1-50-50-900

IDC Benelux (Belgium)
29 Avenue Louis Gribaumont
B-1150 Brussels, Belgium
32-2-779-46-04

IDC Benelux (The Netherlands)
A. Fokkerweg 1
1059 CM Amsterdam
The Netherlands
31-20-669-2721

IDC Central Europe (ECE)
Male Namesti 13
Praha 1 110 00, Czech Republic
420-2-2142-3140

IDC Central Europe (Germany)
Nibelungenplatz 3, 11th Floor
60318 Frankfurt, Germany
49-69-90502-0

IDC Central Europe (Switzerland)
Niederlassung Züerich
WTC, Leutschenbachstrasse 95
CH - 8050 Züerich
Switzerland
41-1-307-1000

IDC Egypt
39 Iraq Street
Mohandesseen, Cairo, Egypt
20-2-336-7355

IDC France
Immeuble La Fayette
2, Place des Vosges, Cedex 65
92051 Paris la Defense 5, France
33-14-904-8000

IDC Hungary
Bajcsy-Zsilinszky út. 57
Building 3, Rooms 103-104
H-1065 Budapest, Hungary
36-1-153-0555/ext. 165, 166

IDC Israel
4 Gershon Street
Tel Aviv 67017, Israel

IDC Italy
Viale Monza, 14
20127 Milano, Italy
390-2-284-571

IDC Nigeria
House 2, 'C' Close
403 Road, 4th Avenue
New Extension, Festac Town
Lagos, Nigeria
234-1-883585

IDC Nordic (Denmark)
Jagtvej 169B
DK-2100 Copenhagen, Denmark
45-39-162222

IDC Nordic (Finland)
Jarrumiehenkatu 2
FIN-00520
Helsinki, Finland
358-9-8770-466

IDC Nordic (Sweden)
Box 1096 Kistagången 21
S-164 25 Kista, Sweden
46-8-751-0415

IDC Poland/ProMarket
Wrobla 43
02-736 Warsaw, Poland
48-22-644-4105

IDC Portugal
Av. Antonio Serpa, 36 Piso 9
1050-027 Lisbon
Portugal
351-21-796-5487

IDC Russia
c/o PX Post, RDS 186
Ulitsa Zorge 10
Moscow 125525
Russian Federation
7-501-929-9959

IDC South Africa
c/o BMI-TechKnowledge
3rd Floor, 356 Rivonia Blvd.
PO Box 4603, Rivonia, 2128
South Africa
27-11-803-6412

IDC Spain
Ochandiano, 6
Centro Empresarial El Plantio
28023 Madrid
34-91-7080007

IDC Turkey
Tevfik Erdonmez Sok. 2/1 Gul Apt.
Kat 9D; 46 Esentepe
Istanbul, Turkey
90-212-275-0995

IDC U.K.
British Standards House
389 Chiswick High Road
London W4 4AE
United Kingdom
44-20-8987-7100

LATIN AMERICA

IDC Miami
Latin America Headquarters
5301 Blue Lagoon Drive
Suite 490
Miami, FL 33126
305-267-2616

IDC Argentina
Trends Consulting
Rivadavia 413, 4th Floor, Suite 6
C1002AAC, Buenos Aires, Argentina
54-11-4343-8899

IDC Brasil
Alameda Ribeirão Preto, 130 cj 41
01331-000 São Paulo
SP Brazil
55-11-253-7869

International Data Corp. Chile
Luis Thayer Ojeda 166 Piso 12
Providencia, Santiago 9, Chile
56-2-231-0111

IDC Colombia
Carrera 40 # 103-78
Bogota, Colombia
571-533-2326

IDC Mexico
Select - IDC
Av. Nuevo Leon No. 54 Desp. 501
Col. Hipodromo, Condesa
C.P. 06100 Mexico, D.F.
52-5-256-1426

IDC Venezuela
Calle Guaicapuro
Edif. Torre Seguros Alianza
Piso 6, Ofc. 6-D, El Rosal
Caracas 1060, Venezuela
58-2-951-3270

IDC delivers accurate, relevant, and high-impact data and insight on information technology to help organizations make sound business and technology decisions. IDC forecasts worldwide IT markets and adoption and technology trends, and analyzes IT products and vendors, using a combination of rigorous primary research and in-depth competitive analysis. IDC is committed to providing global research with local content through more than 500 analysts in more than 40 countries worldwide. IDC's customers comprise the world's leading IT suppliers, IT organizations, and the financial community. Additional information on IDC can be found on its Web site at http://www.idc.com.

IDC is a division of IDG, the world's leading IT media, research, and exposition company.

IDC
Analyze the Future

IDC
5 Speen Street • Framingham, MA 01701
(508) 872-8200 • Fax (508) 935-4015 • www.idc.com

00-282SYSTEM2816